OneSpan

CASE STUDY
ODEABANK

EXECUTIVE SUMMARY

Business Objectives

- Improve the customer experience and protect against fraud by integrating software authentication with the mobile banking app

The Challenge

- Help prevent SIM swap fraud
- Regulatory compliance

The Solution

- Expand the use of one-time passcodes (OTP) delivered by push notification – instead of SMS

Results

- Positive feedback from customers
- Capture fraud attempts before customers are harmed
- Compliance with new regulation in Turkey

odeabank

PROVIDES A SEAMLESS EXPERIENCE WITH INTEGRATED SOFTWARE AUTHENTICATION ON THEIR MOBILE BANKING APP

How the bank improved user experience and security, while reducing SIM swap and other fraud attacks

Odeabank entered the Turkish banking market in 2012 as a subsidiary of Bank Audi Group. This dynamic and innovative bank ranks in the top 10 private sector deposit banks in the country in terms of total assets. Today, 90% of the bank's transactions flow through the digital channels and therefore strong customer authentication remains a top priority in the fight against social engineering and other types of fraud.

Two years after establishing operations in Turkey, the bank integrated the OneSpan Mobile Security Suite with their mobile banking app. Mobile Security Suite is a software development kit (SDK) that provides all the necessary building blocks to protect a mobile application while reducing development overhead. It also enables support for a wide range of authentication options, such as one-time passcodes (OTP), out-of-band push notifications, and biometrics.

As an innovator, it was always important for Odeabank that the digital banking experience be easy and convenient – but above all else, it had to be secure. The bank saw software authentication as the best of both worlds. To introduce it to their retail and corporate banking users, the bank first integrated it with their mobile banking app. Soon after, they extended it so customers could use the software OTP as a second factor of authentication when logging in to online banking as well.

"Rather than having a single OTP application in the app stores as most of our competitors preferred, we integrated the OTP feature into the Odeabank mobile banking app," says Sinan Erdem Özer, Odeabank's Chief Operating Officer. "The integrated authentication was always a strategic part of the customer experience, because every time a customer interacts with the mobile app or Internet banking, the first thing they do is authenticate. That had to be seamless, right from the start."

> "Strong authentication is crucial, especially considering that 90% of retail and commercial banking transactions go through our digital channels. Our duty is to protect our customers' data, wealth, and access to our channels – and OneSpan helps us do that."
>
> **Sinan Erdem Özer**
> Odeabank's Chief Operating Officer

To get started, the user experience is simple. Customers activate their mobile app by providing their phone number and internet banking username/password. After activation, they log in to the mobile app by entering the password they created during the activation session. From that point forward, the app automatically generates and sends the OTP to the back-end system, providing users with easy access to their accounts in seconds. Customer feedback was very positive. “Once customers start using it, they never go back – just because it’s such a good experience.”

The bank’s goal was to create a seamless omni-channel authentication experience across mobile banking, online banking, ATMs, and the contact center. The bank also began to study and compare the effectiveness of software OTP against other methods of authentication.

SMS-OTP (Reactive Security) vs. Integrated OTP with Push Notifications (Proactive Security)

While SMS authentication is a popular authentication method in Turkey, the bank believed that the integrated software authentication was more secure than delivering the OTP via SMS. SMS-OTP is vulnerable to attacks, and banks have to manage risks related to phishing and other types of social engineering attacks, such as SIM swap fraud.

“Once the fraudster has the SIM card in their possession, they can take over the customer’s account. That’s when it becomes a reactive approach on our behalf to catch these incidents, notify the customer, and take action to protect them.”

Using OneSpan’s solution, what the bank found is that the software OTP shifts the authentication from the SIM card to the phone. Even if an attacker successfully takes over a customer’s SIM card, the fraudster is not able to receive an authentication code since a push notification would only be sent to the app on the device registered by the legitimate user. OneSpan binds the authenticator functionality to the registered user’s device, to ensure that only the app installed on the registered device will generate valid OTPs.

“By using their device as the authentication method, we can reduce SIM swap attacks. We still need to be careful, because malicious actors are always looking for new ways to perpetrate fraud, but we definitely see the integrated authentication with push notifications as more secure. We had a chance to watch and explore that in the last five years of our partnership with OneSpan.”

When Odeabank first introduced the integrated OTP functionality, they did so with several thousand customers to start. This gave the bank the opportunity to compare (both from a security and user experience perspective) against a different pool of customers using SMS-OTP.

“As we observed both the test group (who had received the integrated software authentication) and the control group (using the SMS-OTP) we identified several important differences. One being that the telecom industry is regulated differently from the banking sector, and there are challenges there related to stopping SIM swap fraud before the fraudsters can access our customers’ accounts.”

“With OneSpan’s integrated authentication solution, we could capture fraud attempts before the customer was harmed financially or otherwise. That was a significant motivator for us to invest more in the software OTP solution,” says Mr. Özer.

New Regulation Moves the Industry Away from SMS-OTP

In 2020, Odeabank expanded the number of software authentication licenses more than five-fold. Today, 90% of their online banking users also use the mobile app. With such strong mobile adoption, security has become an even more critical aspect of the digital customer experience.

While the bank was already planning to expand the software authentication to more customers and use cases, this decision was accelerated by the new regulation in Turkey. Turkey’s Regulation on Information Systems of Banks and Electronic Banking Services entered into force on 1 July 2020. It addresses information security for banks and electronic banking services. Each banking channel is subject to detailed regulations in terms of authentication and transaction security. For example, Article 34 mandates that customers use two-factor authentication (2FA) for account access and transactions, across the online, mobile, telephone, and ATM channels.

The regulation also addresses concerns regarding the security issues associated with SMS-OTP. Banks cannot send an OTP via SMS to authorize any transactions during the session or use it as an authentication element.

“With the new regulation in Turkey, we see this shifting the banks away from using the telecom industry as an authentication provider toward more secure solutions like software OTP.”

Swapping a SIM card is a legitimate service offered by mobile phone operators when a customer switches to a new device and the old SIM card is no longer compatible.

Fraudsters can abuse this service. While the fraud requires research and preparation, the hack itself is relatively simple. In a SIM swap scam, criminals use social engineering techniques to transfer the victim’s mobile number to a new SIM card. All of the victim’s SMS messages are then redirected to the fraudster.

This enables the fraudster to target banking solutions that use the mobile phone as part of the authentication flow. For example, if enrollment of a mobile banking app happens through SMS, fraudsters can use SIM swapping to impersonate the victim and activate the banking app on the fraudster’s phone.

Also, if the bank’s authentication mechanism includes text messages as a means of delivering one-time passcodes, then taking over the victim’s number becomes an attractive way for a criminal to authenticate fraudulent transactions.

Expanding to Future Use Cases

As a next step, Odeabank is planning to roll out the software authentication to the larger customer base, to provide a consistent authentication experience across channels and use cases. But first, the bank is performing user group studies that will help them redesign certain user experiences.

"For example, right now we already have a customer base using the OneSpan solution. Some like the fact that they set a 6-digit code and enter it, in addition to their password. This group of customers finds it more secure. But others find it redundant. They would rather have a seamless login experience without putting in a password. They prefer the authentication happen entirely on the backend. So we are observing customer behaviors to determine whether we still need to offer both options."

These customer insights will influence the next iterations of the customer authentication experience across channels.

> From the first interaction with the customer, if they are new to the bank, or want to do a transaction during the day, we make it seamless in every way. The OneSpan solution enables us to offer an omni-channel experience for non-mobile transactions – meaning if the client uses the mobile app, they can use the software authentication for any kind of transaction across channels. Having mobile as an authentication method helps the customers as well, because they don't need to carry a hardware token."
>
> **Sinan Erdem Özer**
>
> Odeabank's Chief Operating Officer

Conclusion

Odeabank's core banking system is outsourced. As a new bank that started from scratch in 2012, Odeabank found that to penetrate the Turkish market quickly, outsourcing was the most sustainable and flexible approach. The bank continues to pursue the same operational model today. "As a result, our team is used to working remotely with software vendors and local partners. OneSpan and our local partner Komtera Teknoloji deliver without any problems and in a timely manner," says Mr. Özer.

"While we did evaluate other providers, OneSpan has a true value proposition in terms of technology and customer service. OneSpan provides extended service – not only in terms of addressing our needs, but by bringing new ideas on how to get more from the SDKs we already have, without adding costs."

"We think that OneSpan, because of its already established footprint in Turkey, definitely sets the bar in terms of technologies that it provides, and it's not only software OTP solutions, but also other technologies that we can eventually integrate if we want to, like electronic agreements, app shielding, and other solutions. And we look forward to a long-term relationship together."

To learn more about mobile authentication as well as compliance with Turkey's Regulation on Information Systems of Banks and Electronic Banking Services, visit OneSpan.com or contact us to speak to a representative.

OneSpan

OneSpan enables financial institutions and other organizations to succeed by making bold advances in their digital transformation. We do this by establishing trust in people's identities, the devices they use, and the transactions that shape their lives. We believe that this is the foundation of enhanced business enablement and growth. More than 10,000 customers, including over half of the top 100 global banks, rely on OneSpan solutions to protect their most important relationships and business processes. From digital onboarding to fraud mitigation to workflow management, OneSpan's unified, open platform reduces costs, accelerates customer acquisition, and increases customer satisfaction.

CONTACT US
For more information:
info@OneSpan.com
www.OneSpan.com

Last Update October 2020.